REMARKS

Reconsideration of the rejections set forth in the Office action dated 8/30/2002 is respectfully requested under the provisions of 37 CFR §1.111(b).

Applicant hereby petitions for a one month extension.

Claims 1-24 are pending.

Claims 1-24 have been rejected.

Claims 1-5, 8-13, 15-19 and 22-24 were amended. These claims were amended to make them more clear and definite. The amendments to the independent claims are broadening amendments submitted to more fully claim that which is applicant's invention, and are not intended to limit or narrow the scope of the claims or to effect the Doctrine of Equivalents as it might be applied to the claims, were they unamended. The amended dependant claims were amended to conform to the changes in their independent claims. Additional amendments are subsequently described.

Drawings

The Examiner has properly objected to the missing drawings. After a review of our files, applicant believes that Figures 1A-1C were not sent with the application by the patent firm who wrote this application. Applicant includes herewith a proposed drawing correction that includes the missing figures. Figure 1B is described in the specification at page 11, lines 2-11. Figure 1C is described in the specification at page 11, lines 13-22. No new matter was added by the proposed Figures 1B and 1C as the text clearly describes what these proposed figures show. Thus, proposed Figure 1B and 1C simply conform to the specification.

Figure 1A is described starting at page 9, line 31 through page 11, line 2 -- and in the context established at page 8, line 23 through page 9, line 31. Applicant's current attorney assigned the task of recreating Figure 1A to another patent attorney, Mr. Daniel B. Curtis, reg: 39,159. According to Mr. Curtis' affidavit filed herewith, Mr. Curtis read the specification, and prior to discussing the issue with the inventors, used the specification and his own understanding of the technology to conceptualize the cryptoserver architecture. Mr. Curtis reduced his

conceptualization to proposed Figure 1A and verified his conceptualization of the system architecture with Inventor Smetters. Mr. Curtis is no more than skilled in the art. Thus, no new matter was added by proposed Figure 1A because the proposed figure is supported either directly or inherently, by the originally filed specification, drawings, or claims as interpreted by one skilled in the art and because proposed Figure 1A merely clarifies or completes the original disclosure.

I. Objections

Claim 15 was objected to. The claim was amended to address the objection.

II. Rejections under 35 USC § 112, 2nd Paragraph

Claim 24 stands rejected as being indefinite. Claim 24 was amended to make it a system claim depending from claim 20 and to provide sufficient antecedent basis for the limitation.

III. Rejections under 35 USC §102(e)

Claims 1-5, 9, 11-13, 15-19 and 23 stand rejected as being anticipated by Yamamoto (6,078,663).

Applicant respectfully traverses this rejection as a prima facie case of anticipation has not been made because Yamamoto does not teach or enable each of the claimed elements as interpreted by one of ordinary skill in the art.

Amended claim 1 is directed to a method for pricing a cryptographic service (for example, but without limitation, a service for encrypting data). A user who desires to off-load a cryptographic operation from the user's computer can select a cryptographic service provider to perform the cryptographic operation for the user (by selecting the appropriate cryptographic service). The cryptographic service provider receives a request for the desired service and generates a contract based on a variable pricing scheme and sends the contract to the user. The user can then determine whether or not to use that cryptographic service provider to perform the desired cryptographic operation.

This aspect of the invention is captured in amended Claim 1:

A method for pricing a cryptographic service on a network utilizing one or more

cryptoservers, comprising:

(a) receiving a request for the cryptographic service from a user utilizing the network, wherein the request is received by a cryptographic service provider;

(b) generating a contract based on a variable pricing scheme in response to the request; and

(c) sending the contract from the cryptographic service provider to the user utilizing the network.

Yamamoto teaches techniques for distributing encrypted information from an information providing center to a user who has agreed to a fee for the providing of the information as well as the strength of the encryption used to protect the provided information. As such, Yamamoto is a provider of encrypted data. Thus, the user is simply contracting for access to encrypted information stored at the providing center. This is completely different from the claimed invention where the user is requesting pricing for a cryptographic service to be performed by the cryptographic service provider.

In one aspect of the invention of amended claim 1, the cryptographic service provider provides a cryptographic service to the user. For example, where the cryptographic service performs a data encryption operation, the user's client computer generates a tunnel on the network, sends information necessary for the cryptographic service to perform the data encryption operation (for example, the data to be encrypted and a key), waits, and then receives the encrypted data. Thus, the user's computer need not perform the cryptographic operation as the service provider's cryptographic service performs that operation for the user for a price.

Amended claim 1 is directed towards the cryptographic service provider offering the cryptographic service desired by the user for a price. Because the cryptographic service is valuable and because there may be multiple cryptographic service providers who provide different terms and prices for the desired cryptographic service, the service provider provides a contract offering the desired cryptographic service and sends that contract to the user.

Yamamoto's technology simply provides encrypted information from an information provider. Yamamoto discloses a file server that is enhanced to provide encryption to the

information in the served files and where a user can select a trade-off between the strength of the encryption, the amount of time it takes to provide the encrypted data, and the user's cost.

The invention of amended claim 1 provides an encryption service for a user and this is completely different from Yamamoto's encrypted file server. Thus, Yamamoto does not teach or enable each of the claimed elements as interpreted by one of ordinary skill in the art; and amended **claims 1, 11 and 15**, are not anticipated by Yamamoto.

Amended **claims 2-5 and 9** depend on and further limit claim 1 (either directly or through intervening claims). Thus, these claims are also not anticipated.

Amended **claims12-13** depend on and further limit claim 11. Thus, these claims are also not anticipated.

Amended **claims 16-19 and 22-24** depend on and further limit claim 15 (either directly or through intervening claims). Thus, these claims are also not anticipated.

Further, with regards to Claims 3 and 17, applicant traverses the assertion that Yamamoto teaches that the plurality of cryptoservers are commercial services that compete for customers. Yamamoto simply teaches that one of a selection of enciphering systems (having different levels of encrypting strength) provided by the same information providing center can be selected by a user. There is no competition for customers. Instead a single customer is able to trade off the price of the data with how strong and how fast the data provided by the information providing center will be encrypted. The customer who has selected the information providing center simply selects what level of encryption is desired for the information by selecting which enciphering system to use.

IV. Rejections under 35 USC §103(a)

Claims 6-8, 14, 20-22 and 24 stand rejected under 35 USC §103 as being unpatentable over Yamamoto in view of Coyle (6,269, 157). This rejection is respectfully traversed in view of the following arguments.

These claims depend on and further limit (either directly or through intervening claims) amended **claims 1, 11, and 15**.

Yamamoto has been previously discussed in section III.

Coyle teaches a computerized bidding system for selecting telecommunication carriers.

Amended claims 1, 11 and 15 are patentable over both Yamamoto and Coyle either separately or combined because these references would not teach a suggestion or modification that would appear to be sufficient to have made the invention of amended claim 1, 11 or 15 obvious to one of ordinary skill in the art because the combination of these references would only teach an encrypted file provider that has bidding capability instead of an encryption service.

Amended **claims 6-8, 14, 20-22 and 24** depend on (either directly or through intervening claims) independent amended claims 1, 11, or 15. Thus amended claims 6-8, 14, 20-22 and 24 are also patentable.

Amended **claim 10** stands rejected under 35 USC §103 as being unpatentable over Yamamoto in view of Schneier et al. (5,596,404). This rejection is respectfully traversed in view of the following arguments.

Yamamoto has been previously discussed in section III.

Schneier teaches a method of creating a digital signature.

Claim 10 depends on (through interveaning claims) and further limits claim 1 that is patentable. Thus, claim 10 is patentable.

In view of the foregoing remarks, reconsideration of this application and allowance thereof are earnestly solicited. In the event the Examiner considers a personal contact advantageous to the disposition of this case, the Examiner is hereby requested to call Attorney for Applicant(s),

Respectfully submitted,

Richard B. Domingo
Attorney for Applicant(s)
Registration No. 36,784
Telephone: 650-812-4269

Palo Alto, California
Date: 12/20/2002

Version with markings to show changes made

1.(amended) A method for pricing a cryptographic service on a network utilizing ~~at least~~ one ~~cryptoserver~~or more cryptoservers, comprising:

(a) receiving a request for ~~a~~the cryptographic service from a user utilizing ~~a~~the network, wherein the request is received by a cryptographic service provider;

(b) generating a contract based on a variable pricing scheme in response to the request; and

(c) sending the contract from the cryptographic service provider to the user utilizing the network.

2.(amended) The method as recited in claim 1, wherein the cryptographic service provider selects one of ~~a plurality of~~the one or more cryptoservers to perform the cryptographic service.

3.(amended) The method as recited in claim 2, wherein the ~~plurality of cryptoservers are~~cryptographic service provider is a commercial service~~s~~ competing for customers.

4.(amended) The method as recited in claim 2, wherein the ~~plurality of~~one or more cryptoservers ~~are~~is part of a single distributed service.

5.(amended) The method as recited in claim 1, wherein the variable pricing scheme is based on at least one of~~:~~ a data load of ~~computational burden of a cryptoserver~~ the one or more cryptoservers during performance of the cryptographic service, a distance between the ~~cryptoserver~~one or more cryptoservers and the user, a congestion of the network during performance of the cryptographic service, and a rating of the ~~cryptoserver~~one or more cryptoservers performing the cryptographic service.

8.(amended) The method as recited in claim 6, wherein ~~a plurality of~~ the one or more cryptoservers bid for providing the cryptographic service.

9.(amended) The method as recited in claim 1, wherein the cryptographic service provider is ~~a cryptoserver.~~one of the one or more cryptoservers.

10.(amended) The method as recited in claim ~~1~~3, wherein the cryptographic service provider provides a receipt upon performing the cryptographic service, wherein the receipt includes at least one of a one-way hash of the results of its computations, the time and duration of the computations, a description of the computations, and the identities of the ~~cryptoserver~~one or more cryptoservers and the customer.

11.(amended) A computer program embodied on a computer readable medium for pricing a cryptographic service on a network utilizing ~~at least one cryptoserver~~one or more cryptoservers, comprising:

(a) a code segment that receives a request for ~~a~~the cryptographic service from a user utilizing ~~a~~the network, wherein the request is received by a cryptographic service provider;

(b) a code segment that generates a contract based on a variable pricing scheme in response to the request; and

(c) a code segment that sends the contract from the cryptographic service provider to the user utilizing the network.

12.(amended) The computer program as recited in claim 11, wherein the cryptographic service provider selects one of ~~a plurality of~~the one or more cryptoservers to perform the cryptographic service.

13.(amended) The computer program as recited in claim 11, wherein the variable pricing scheme is based on at least one of a data load of ~~a cryptoserver~~the one or more cryptoservers during performance of the cryptographic service, a distance between the ~~cryptoserver~~one or more cryptoservers and the user, a congestion of the network during performance of the cryptographic service, and a rating of the ~~cryptoserver~~one or more cryptoservers performing the cryptographic service.

15.(amended) A system for pricing a cryptographic service ~~on a network utilizing at least one cryptoserver,~~ comprising:

(a) a network;

(b) ~~a cryptoserver~~ one or more cryptoservers for providing a cryptographic service;

(c) logic that receives a request for the cryptographic service from a user utilizing the network, wherein the request is received by a cryptographic service provider;

(~~b~~d) logic that generates a contract based on a variable pricing scheme in response to the request; and

(~~c~~e) logic that sends the contract from the cryptographic service provider to the user utilizing the network.

16.(amended) The system as recited in claim 15, wherein the cryptographic service provider selects one of ~~a plurality of~~the one or more cryptoservers to perform the cryptographic service.

17.(amended) The system as recited in claim 16, wherein the ~~plurality of cryptoservers are~~ cryptographic service provider is a commercial service~~s~~ competing for customers.

18.(amended) The system as recited in claim 16, wherein the ~~plurality of~~one or more cryptoservers ~~are~~is part of a single distributed service.

19.(amended) The system as recited in claim 15, wherein the variable pricing scheme is based on at least one of: data load of ~~a cryptoserver~~the one or more cryptoservers during performance of the cryptographic service, a distance between the ~~cryptoserver~~one or more cryptoservers and the user, a congestion of the network during performance of the cryptographic service, and a rating of the ~~cryptoserver~~one or more cryptoservers performing the cryptographic service.

22.(amended) The ~~method~~system as recited in claim 19, wherein ~~a plurality of~~the one or more cryptoservers bid for providing the cryptographic service.

23.(amended) The ~~method~~system as recited in claim 15, wherein the cryptographic service provider is ~~a cryptoserver.~~one of the one or more cryptoservers.

24.(amended) The ~~method~~system as recited in claim ~~1~~20, wherein the auction-based variable pricing scheme is conducted securely as a cryptographic protocol by some of the one or more cryptoservers.